



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/734,083

12/11/2003

Richard Lippmann

MIS-00301

7971

22494

7590

06/16/2006

DALY, CROWLEY, MOFFORD & DURKEE, LLP  
SUITE 301A  
354A TURNPIKE STREET  
CANTON, MA 02021-2714

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/734,083	LIPPMANN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 08 May 2006.
- 2a) ☐ This action is FINAL.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 117-174 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 117-174 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>20060411</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2137

**DETAILED ACTION**

1. Claims 117-174 are pending.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/08/2006 has been entered.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 137-138, 145, 166-167 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. Claims 137, 145, and 166 provides for the use of the attack tree and vulnerability data, but, since the claim does not set forth any steps involved in the method/process, it is unclear

Art Unit: 2137

what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

6. Any claims not specifically addressed are rejected by virtue of their dependencies.

***Claim Rejections - 35 USC § 101***

7. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 137-138, 145, 166-167 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd. v. Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

Art Unit: 2137

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 117-126, 130-145, 146-155, 159-174 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al (US 6952779) in view of Steffan et al ("Collaborative Attack Modeling").

As per claims 117 and 146, Cohen et al discloses using a computer to generate a attack graph, using the computer comprises: designating a root node of the attack graph, the root node representing a starting point of an attack (see figure 5 and column 17 line 44 through column 18 line 4); and for a current node included in the pruned attack tree, connecting a resulting node having a first state and an edge having a first transition value to the current node (see column 6 lines 25-53).

Cohen et al fails to disclose a pruned attack tree and connecting nodes using an edge if another edge having a second transition value does not connect an ancestor of the current

Art Unit: 2137

node to another node having a second state equivalent to the first state; and the second transition value is equal to the first transition value.

However, Steffan et al teaches pruning an attack tree with such properties (see section 3.1 and section 5).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to prune Cohen et al's attack tree.

Motivation to do so would have been that it is advantageous to prune non-relevant sub-graphs when a condition is not fulfilled (see section 5).

As per claims 118 and 147, the modified Cohen et al and Steffan et al system discloses the pruned augmented attack tree is a tree including n levels, said starting point being a root of said tree at level 0, n being at least 0 (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 119 and 148, the modified Cohen et al and Steffan et al system discloses said pruned augmented attack tree represents information about at least one of: an attacker state including a host and an attacker access level on said host, and a network state (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 120 and 149, the modified Cohen et al and Steffan et al system discloses an edge from a first node at level  $x$  to a second node at level  $x+1$  represents an action while in a first state including a first attacker state corresponding to said first node resulting in a second state including a second attacker state (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 121-122 and 150-151, the modified Cohen et al and Steffan et al system discloses said action exploits a vulnerability on a host in said network wherein said first attacker state represents a first host and a first attacker access level on said first host, and said second attacker state represents at least one of: a second host and a second attacker access level on said second host, and said first host and a second attacker access level on said first host wherein said second attacker access level represents at least one of: an increase in attacker privilege, an increase in attacker access, and an increase in attacker knowledge (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 123-124 and 152-153, the modified Cohen et al and Steffan et al system discloses said current node is at a level  $n$ , and said ancestors of said current node are located at levels in said pruned augmented attack tree at a level less than

Art Unit: 2137

n and said pruned augmented attack tree is generated using a breadth first search technique in which nodes are added to said pruned augmented attack tree at an nth level prior to adding any node from level n+1 to said pruned augmented attack tree (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 125 and 154, the modified Cohen et al and Steffan et al system discloses a plurality of computer attack paths for said network are represented using a plurality of pruned augmented attack trees, each of said pruned augmented attack trees representing computer attack paths originating from a unique starting point (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 126 and 155, the modified Cohen et al and Steffan et al system discloses said starting point is one of: from within said network and external to said network (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 130 and 159, the modified Cohen et al and Steffan et al system discloses said generating uses connectivity information, said connectivity information including a connection between two endpoints representing elements of a configuration of said network (see Cohen et al figure 5 and



Art Unit: 2137

column 17 line 44 through column 18 line 4; column 6 lines 25-67 and Steffan section 3.1).

As per claims 131 and 160, the modified Cohen et al and Steffan et al system discloses said connectivity information includes physical connectivity between network interfaces and logical connectivity through network communications protocols (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4; column 6 lines 25-67 and Steffan section 3.1).

As per claims 132-133 and 161-162, the modified Cohen et al and Steffan et al system discloses said connection is associated with a path including one or more hops wherein each of said one or more hops is associated with at least one of: a filtering rule, a translation rule, and an interface of a host in said network (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4; column 6 lines 25-67 and Steffan section 3.1).

As per claims 134-136 and 163-165, the modified Cohen et al and Steffan et al system discloses at least one of said endpoints is associated with a vulnerability on said at least one endpoint wherein said vulnerability has an associated action resulting in exploitation of said vulnerability wherein said associated action is related to an entity representing at least one of: an attacker access level, attacker knowledge level, a

Art Unit: 2137

change to a network state (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

As per claims 137-138 and 166-167, he modified Cohen et al and Steffan et al system discloses said pruned augmented attack tree is used to determine an effect of preventing at least one action and modifying said pruned augmented attack tree in accordance with eliminating at least one action in connection with a vulnerability associated with said host producing a modified augmented attack tree; and evaluating said modified augmented attack tree (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4 and column 9 lines 23-43).

As per claims 139 and 168, the modified Cohen et al and Steffan et al system discloses connectivity data representing connectivity between pairs of endpoints in said network is used by said generating, and the method further comprising: automatically generating said connectivity data in accordance with at least one translation rule, at least one filtering rule, and network configuration information (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4 and Steffan section 3.1).

As per claims 140 and 169, the modified Cohen et al and Steffan et al system discloses said at least one translation rule includes at least one of: an address translation rule and a

Art Unit: 2137

port translation rule (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4 and Steffan section 3.1).

As per claims 141 and 170, the modified Cohen et al and Steffan et al system discloses selecting at least one address of a starting point of a computer attack using at least one rule; and determining a portion of said connectivity data using said at least one address (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4 and Steffan section 3.1).

As per claims 142-144 and 171-173, the modified Cohen et al and Steffan et al system discloses said at least one rule includes at least one of a filtering rule and a translation rule and said at least one address is used in said generating to represent an alternate connectivity of a host said address is one of an address in accordance with a communications protocol and an address associated with said network (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4 and Steffan section 3.1).

As per claims 145 and 174, the modified Cohen et al and Steffan et al system discloses using vulnerability data to determine at least one of: requirements for an action, an attacker state resulting from an action, and a network state resulting from an action, where said requirements include a locality describing whether a vulnerability can be exploited

Art Unit: 2137

remotely over a network or locally on a host, said resulting attacker state includes an effect describing an access level or privilege or knowledge after an exploit of a vulnerability, and said resulting network state includes a denial of service describing a loss of service on a host after an exploit of a vulnerability (see Cohen et al figure 5 and column 17 line 44 through column 18 line 4).

11. Claims 129 and 158 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Cohen et al and Steffan et al system as applied to claims 1 and 59 above, and further in view of Ammann et al (Scalable, Graph-Based Network Vulnerability Analysis).

As per claims 129 and 158, the modified Cohen et al and Steffan et al system fails to disclose determining which hosts in said network are equivalent forming a group; and representing said group with a single host.

However, Ammann teaches such grouping (see page 223 right column).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to group similar hosts in the modified system of Cohen et al and Steffan et al.

Motivation to do so would have been to simplify the attack graph (see Ammann page 223 right column).

Art Unit: 2137

12. Claims 127-128 and 156-157 are rejected under 35

U.S.C. 103(a) as being unpatentable over the modified Cohen et al and Steffan et al system as applied to claims 6 and 64 above, and further in view of Swiler et al (Computer-Attack Graph Generation Tool).

As per claims 127-128 and 156-157, the modified Cohen et al and Steffan et al system fails to disclose evaluating each action that exploits a vulnerability of a host in accordance with connectivity data wherein said connectivity data, said each action, and said vulnerability are stored in a database and determined prior to performing said generating.

However, Swiler teaches evaluating each action that exploits a vulnerability of a host in accordance with connectivity data (see section 2.2) wherein said connectivity data, said each action, and said vulnerability are stored in a database and determined prior to performing said generating (see sections 3.1 and 3.2.1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Swiler's data collection and storing method in the modified system of Cohen et al and Steffan et al.

Motivation to do so would have been that commercial tools primarily use databases to store results (see section 3.2.1).

***Response to Arguments***

13. Applicant's arguments with respect to claims 117-174 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Mahieu (US 20060015943), Basu et al. (US 6836888), Swiler et al (US 7013395), and Tidwell et al teach methods of generating attack trees.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER